Joint Data Decoding and RF Jamming Detection in Cooperative Wireless Vehicular Networks

Ταυτόχρονη Αποκωδικοποίηση Δεδομένων και Ανίχνευση Παρεμβολών σε Συνεργατικά Δίκτυα Οχημάτων

Master Thesis
by
Savvas Chatzisavvas

University of Thessaly
Department of Electrical and Computer Engineering

Supervisors:

Argyriou Antonios
Korakis Athanasios
Potamianos Gerasimos

Volos, October 2018

Acknowledgments

I would like to thank my supervisor Dr. Argyriou Antonios who gave me the motivation and inspiration to move on and complete my study.

Dedicated to my family.

Abstract

In this thesis we are concerned with the problem of RF jamming of a moving swarm of wireless communicating nodes. In our system model a swarm of nodes receive an information signal from a master node, that they want to decode, while the RF jammer desires to disrupt this communication. For this system model we propose a transmission scheme where the master node remains silent for a time period while it transmits in a subsequent slot. For this transmission scheme we present a joint data and jamming signal estimation algorithm that uses Linear Minimum Mean Square Error (LMMSE) estimation. We develop analytical close-form expressions that characterize the Mean Square Error (MSE) of the data and jamming signals. Our numerical results for different system configurations prove the ability of our overall system to combat RF jamming effectively.

Περίληψη

Σε αυτή τη διπλωματική ασχολούμαστε με το πρόβλημα της RF παρεμβολής σε ένα κινούμενο σμήνος κόμβων που επικοινωνούν ασύρματα μεταξύ τους. Στο μοντέλο του συστήματος μας, ένα σμήνος από κόμβους δέχεται ένα σήμα πληροφορίας από έναν κύριο κόμβο προσπαθώντας να το αποκωδικοποιήσει, ενώ ένας RF παρεμβολέας επιθυμεί να διακόψει αυτή την επικοινωνία. Για αυτό το μοντέλο συστήματος προτείνουμε ένα σύστημα μετάδοσης όπου ο κύριος κόμβος παραμένει σιωπηλός για ένα χρονικό διάστημα και μεταδίδει σε μια επόμενη χρονική στιγμή. Για αυτό το σύστημα μετάδοσης παραθέτουμε έναν αλγόριθμο εκτίμησης του σήματος παρεμβολής και της κοινής πληροφορίας χρησιμοποιώντας τον Γραμμικό Εκτιμητή Ελάχιστου Τετραγωνικού Σφάλματος (LMMSE). Αναπτύσσουμε μία κλειστή μορφή εξισώσεων του Μέσου Τετραγωνικού Σφάλματος τόσο για τα δεδομένα όσο και τα σήμα της παρεμβολής. Τέλος τα αριθμητικά μας αποτελέσματα για διαφορετικές διαμορφώσεις του συστήματος μας, αποδεικνύουν την συνολική ικανότητα του συστήματος να καταπολεμά τις RF παρεμβολές αποτελεσματικά.

Contents

List of Figures

Chapter 1

Introduction

Wireless communication is characterized by a vulnerable medium that has constraints in power, bandwidth and communication range. As the ulitily and usefulness of these networks increases every day, more and more malicious competitors show up and target these networks with different security attacks. RF Jamming is one method that a malicious node can use to disrupt the transmission between the nodes of a wireless network. In this type of attack a high-power signal is used to disrupt the communication via the vulnerable medium, as most nodes use one single frequency band. In certain application domains where groups of wireless nodes must communicate reliably in broadcast mode, like drone swarms or platoons of autonomous vehicles, an RF jammer can have a profound effect in the operation of the system if it can disrupt wireless communication [1, 2]. There are methods to defend against a jamming attack such as spread spectrum communication, increase of transmission power but they typically incur a high cost (power, bandwidth, or complexity).

Contrary to seeing RF jamming as a problem of an individual node, we propose to address it at the group level since the applications of interest fall into this category. More specifically we propose to use jointly the data from receivers in a swarm of nodes with the purpose of finding a way to estimate and remove the impact of the jamming signal. This will also help to isolate it and estimate better the desirable information signal. To achieve our goal we design a transmission scheme and an associated estimation algorithm. With our protocol in the first time slot the master node does not transmit any useful information so we have a clear observation of the jamming signal with the noise, while in the

second time slot where the desirable signal is transmitted we observe the information signal, the jamming signal, and the noise. Our approach ensures that we have a clean interfering signal. In this work we use the Linear Minimum Mean Square Error Estimator (LMMSE) to estimate both the information signal u and the jamming signal z_i for every node in the swarm i. Our main result is a closed-form expression of the MSE of the signal u and the jamming signal z_i.

The rest of paper is organised as follows: in Section 2 we present related work while in Section 3 we describe our System Setup. In Section 4 we present the proposed the joint data and jamming signal estimation algorithm with the MSE derivations while in Section 5 we present numerical results. Finally in Section 6 we conclude this paper.

Chapter 2

Related Work

Distributed estimation (DES) is a topic that has been considerably in the literature. However, to the best of our knowledge none of these works has been considered using DES in a setting where a jamming signal needs to be estimated. Furthermore, jamming attack detection and mitigation is usually carried out with other methods as we will see next.

One approach [3] is simply trying to avoid the interferer which can be accomplished by either using spectral or spatial evasion (channel surfing and spatial retreats respectively). As a second technique, the author proposed to compete more actively with the interferer by using properly the power levels and coding rate to achieve communication when jammer continues to transmit.

Bahceci et al [5] proposed a method to estimate correlated data in WSNs with optimum power allocation and analog modulation by using two different estimators, the linear unbiased estimator (BLUE) that does not need any information about the correlation matrix and the MMSE estimator that exploits the correlations. They made the comparison between two estimators and shown that MMSE needs lower power to attain the same distorion. The most closely related work is by the authors in [4] where they have implemented a joint Successive Interference Cancellation (SIC) decoder and LMMSE estimator for an interfering (jamming) signal.

Other works focus on using different techniques for combating RF jamming like Multiple Input Multiple Output (MIMO) techniques as an active defence mechanism [1]. They proposed a scheme which combines the well known Alamouti sheme with spatial multiplexing that achieves a higher throughput and robustness for continuous and reactive RF jam-

mers without requiring knowledge for the channel of the jammer. More recent works like [2] propose methods for jamming detection in VANETS with ML methods like clustering. The authors proposed algorithms that can differentiate intentional from unintentional jamming as well as extract specific features of the RF jamming signal. Opeyemi et al. [5] use an EWMA filter to detect the mean shifts in event intensity when jamming attack occurs. EWMA combines both current and previous data to detect small changes in time series with the habit of low or no overload. H. A. Bany Salameh [6] proposed a quality-aware channel assignment algorithm that aims to minimize the invalid ratio of cognitive radio packets transmissions. Their scheme uses the statistical information of primary users regarding the channel conditions like fading and jamming attacks to identify the most reliable channel.

Chapter 3

System Setup

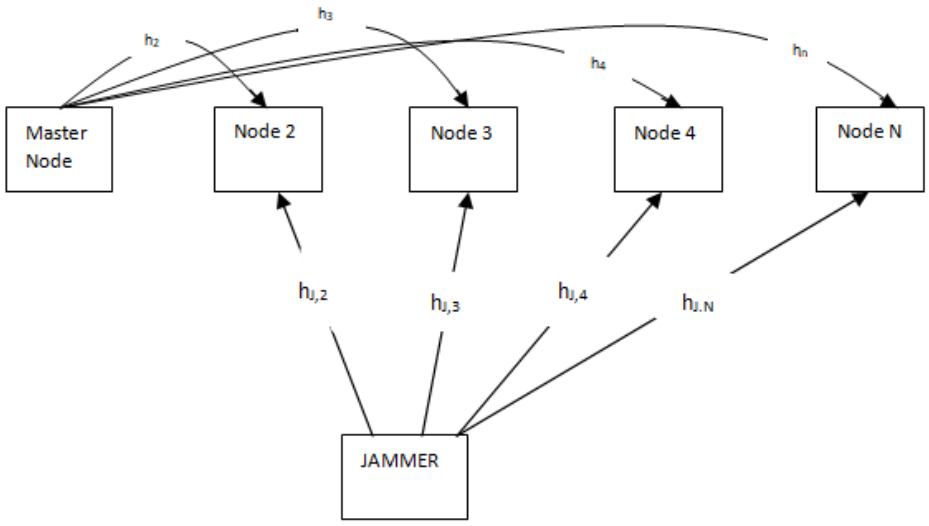

Figure 3.1: Wireless communication network considered in this work.

We consider a wireless communication network that consists of a set of N nodes. The first node is the master node that broadcasts information messages to the remaining $N-1$ nodes, representing thus a typical communication scenario in VANETs and drone swarms. In addition, there is a Jammer (J) who transmits an RF jamming signal that intends to disrupt the communication between the master node and remaining nodes of the network. Each node i observes signal y_{ij}, where i indicates the

node and j the time slot. The master node sends a digitally modulated baseband BPSK signal $u \in \{-1, +1\}$ with zero mean and variance σ_u^2. Of course, for the jamming signal there is no information regarding its mean or variance. We assume that the jammer transmits during the two consecutive time slots in the same way and this means that the jamming signal z is the same. The goal of the network is first to estimate the bit u by removing the jamming signal, and second to estimate the jamming signal at each node independently.

Observation Model. We assume that time is slotted. We design a transmission scheme according to which in one slot the master node transmits bit u and each node i observes the addition of two signals, namely u from the master node through a channel h_i, and one from the jammer through an unknown channel g_i ($z_i = g_i z$). In the second time slot the master node does not transmit anything and each node i observes only the jamming signal z_i. The noise sample w_{ij} for each node and time slot is AWGN with zero mean and variance σ_w^2 and is uncorrelated across the nodes. So the signal model for the two different time slots is:

$$y_{i1} = z_i + w_{i1} \quad \text{(master node does not transmit)} \tag{3.1}$$

and

$$y_{i2} = h_i u + z_i + w_{i2} \quad \text{(master nodes transmits)} \tag{3.2}$$

Hence, the observations form the $2N \times 1$ random vector $\vec{y} = [y_{21} \;\; y_{22} \;\; y_{31} \;\; y_{32} \;\; ... \;\; y_{N1} \;\; y_{N2}]^T$. We can also define

$$\vec{u} = [z_2 \;\; z_3 \;\; z_4 \;\; z_5 \;\; ... \;\; z_n \;\; u]^T$$

$$\vec{w} = [w_{21} \;\; w_{22} \;\; w_{31} \;\; w_{32} \;\; ... \;\; w_{n1} \;\; w_{n2}]^T$$

The final signal model for our system becomes:

$$\vec{y} = H\vec{u} + \vec{w} \tag{3.3}$$

where H is the following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & h_1 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & h_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 1 & h_n \end{bmatrix}$$

Channel Model. For the wireless link we assume flat Rayleigh fading, while the channel remains the same for two consecutive time slots (quasi-static). Hence for every time slot during the transmission of a packet we have $|h_i| \sim Ray(E[|h_i|^2])$ [7]. The average received power that is $E[|h_i|^2] = 1/dist^a$ where $dist$ is the node's distance from the master node and a is the path loss exponent set to 3. We assume that the channel between the master node and the remaining ones is known since it can be easily calculated from packet preambles.

Chapter 4

Joint Data and Jamming Signal Estimation

In this paper we adopt the Linear Mean Square Error Estimator (LMMSE) [8, 9] for estimating the information and the jamming signal. An MMSE estimator is an estimation method which minimizes the mean square error (MSE) which is a common measure of estimator quality. The LMMSE estimator ensures the minimum MSE from all linear estimators. For our general linear model $\vec{y} = H\vec{u} + \vec{w}$, the estimator of $\vec{u}$ is given as:

$$\hat{\vec{u}} = (H^H C_w^{-1} H + C_u^{-1})^{-1} H^H C_w^{-1} \vec{y} \tag{4.1}$$

where $C_{\vec{w}}$ and $C_{\vec{u}}$ are the auto-covariance matrices of $\vec{w}$ and $\vec{u}$ respectively. The MSE of this estimator is the trace of $C_{\vec{e}}$, that is the covariance matrix or the estimation error:

$$MSE = \text{Tr}(C_{\vec{e}}) = \text{Tr}((H^H C_w^{-1} H + C_u^{-1})^{-1})) \tag{4.2}$$

4.1 MSE derivation

As the literature has shown, a very challenging task is to produce a closed-form expression for the desired estimator and signal model [4, 8, 10]. In this subsection we outline the process that has led to the desired expression that will help us study the behavior of the proposed system.

Recall that in our model we assume that the noise is AWGN with zero mean and variance σ_w^2 and is uncorrelated across the nodes. We have no

information about the jamming signal and so we assume that its mean is zero. For the information signal we consider the channels between the master node and the other nodes Rayleigh which has zero mean. Under these assumptions and with the use of the general LMMSE estimator, the MSE for the information u and jamming signal z_i for nodes is given in (4.3), and (4.4) respectively.

$$MSE_u = \frac{1}{\sum_{n=2}^{N}(\frac{h_n^2}{\sigma_{wn2}^2}) + \frac{1}{s_u^2} - \sum_{n=2}^{N}(\frac{h_n^2}{\sigma_{wn2}^4 * (\frac{1}{\sigma_{wn1}^2} + \frac{1}{\sigma_{wn2}^2} + \frac{1}{\sigma_{zn}^2})})} \tag{4.3}$$

In order to understand better the implications of the produced expression we present results for the case of $N = 4$ where we have that

$$MSE_u = \frac{1}{s - \frac{h_2^2}{\sigma_{w22}^4 * \alpha} - \frac{h_3^2}{\sigma_{w32}^4 * \beta} - \frac{h_4^2}{\sigma_{w42}^4 * \gamma}} \tag{4.5}$$

Also MSE_{z2} is equal to

$$\frac{\beta * \gamma * s - \frac{h_3^2}{\sigma_{w32}^4} * \gamma - \frac{h_4^2}{\sigma_{w42}^4} * \beta}{\alpha * \beta * \gamma * s - \frac{h_2^2}{\sigma_{w22}^4} * \beta * \gamma - \frac{h_3^2}{\sigma_{w32}^4} * \alpha * \gamma - \frac{h_4^2}{\sigma_{w42}^4} * \alpha * \beta} \tag{4.6}$$

where:

$$s = \frac{h_2^2}{\sigma_{w22}^2} + \frac{h_3^2}{\sigma_{w32}^2} + \frac{h_4^2}{\sigma_{w42}^2} + \frac{1}{s_u^2}$$

$$\alpha = \frac{1}{\sigma_{w21}^2} + \frac{1}{\sigma_{w22}^2} + \frac{1}{\sigma_{z2}^2}$$

$$\beta = \frac{1}{\sigma_{w31}^2} + \frac{1}{\sigma_{w32}^2} + \frac{1}{\sigma_{z3}^2}$$

$$\gamma = \frac{1}{\sigma_{w41}^2} + \frac{1}{\sigma_{w42}^2} + \frac{1}{\sigma_{z4}^2}$$

The first thing we notice from these expressions is that the MSE of the information signal u is inversely proportional to the number of nodes, that is we have benefits in the accuracy of bit detection (MSE can be easily converted to SNR and BER) when more nodes assist in the estimation process. Regarding the MSE of the estimated jamming signal it is also increased with a higher number of nodes but this is not obvious from the expression that is more involved. The precise quantification of these gains is presented in the next section.

$$MSE_{zi} = \frac{\prod_{n=2,n\neq i}^{N}(\frac{1}{\sigma^2_{wn1}} + \frac{1}{\sigma^2_{wn2}} + \frac{1}{\sigma^2_{zn}}) * (\sum_{k=2}^{N}(\frac{h_n^2}{\sigma^2_{wn2}}) + \frac{1}{s^2_u}) - \sum_{k=2}^{N}(\frac{h_n^2}{\sigma^4_{wn2}}) * \prod_{n=2,n\neq i,k}^{N}(\frac{1}{\sigma^2_{wn1}} + \frac{1}{\sigma^2_{wn2}} + \frac{1}{\sigma^2_{zn}})}{\prod_{n=2}^{N}(\frac{1}{\sigma^2_{wn1}} + \frac{1}{\sigma^2_{wn2}} + \frac{1}{\sigma^2_{zn}}) * (\sum_{n=2}^{N}(\frac{h_n^2}{\sigma^2_{wn2}}) + \frac{1}{s^2_u}) - \sum_{k=2}^{N}(\frac{h_n^2}{\sigma^4_{wn2}}) * \prod_{n=2,n\neq i}^{N}(\frac{1}{\sigma^2_{wn1}} + \frac{1}{\sigma^2_{wn2}} + \frac{1}{\sigma^2_{zn}})} \quad (4.4)$$

Chapter 5

Simulation Results

For our simulation we assume that the master node together with the other nodes form a row of vehicles that move together in a specific direction with a constant velocity. The jammer is in a specific distance and moves in parallel with them but we do not have any information for its position and channel condition between itself and the nodes. Recall that every node knows the channel condition h_i only with the master node. Besides our two-stage transmission scheme we also test a baseline system where the master node transmits data continuously without stopping its transmission as with the proposed scheme. In our analytical model this result can be obtained by setting the noise variance to infinity in (3.1). Furthermore, we assume σ_w^2 to be equal to 0.1. The information signal u is a random binary sequence with power equal to $\sigma_u^2 = 1$ leading thus to a transmit SNR of 10dB. Higher SNRs would lead to higher gains. For the jamming signal note that its variance σ_{zi}^2 at every node takes different values because of channel fading. We implemented our algorithm in Matlab and we executed 50000 iterations for every different system configuration. For our results we present the MSE for the transmitted information u and for the jamming signal z_i.

5.1 Results for an AWGN channel

In figure 5.1 we present the results for the MSE_u and MSE_{zi} for the proposed and baseline systems. We observe that in the baseline system the MSE_u and the MSE_{zi} for $N = 2$ nodes start at the same value. This

is what we expect to observe because only (3.2) is available for u and z_i (and h_i=1). As we add nodes the two MSE's improve and the MSE of the information u enjoys higher improvements with every new node. For the proposed system our results are much better as we have also the observations from the first time slot for every node and we can estimate and isolate better the jamming signal that eventually results in a better estimation of the information u. Although we have better MSE's for both estimated parameters we observe a behavior that requires some further explanation. As we observe in figure 5.1 for the proposed system for a number nodes $N = 2, 3$, the MSE_{zi} is better than the MSE_u. This indicates that one can estimate better the different jamming signal for every node than the common information u for all nodes but this is not the case. The reason for this behavior is that the information signal that we are trying to estimate is common for all nodes but the jamming signal z_i is different for every node and contains the unknown channel h_{ji} and the real jamming term z. So it is easier for us to estimate a range of values z_i than a discrete value u.

5.2 Results for Rayleigh fading channel

When the channels between the master node and the other nodes are Rayleigh fading h_i takes random values. We adopt the same assumptions for the variance of information signal and the noise. In figure 5.2 we present the results for MSE_u and MSE_{zi}. We observe that in the baseline system the MSE is greater than the proposed system because in the baseline system we have only the observations of the second time slot for every node so we do not have the ability to estimate the jamming signal. In both systems the MSE_u that is achieved for $N \geq 4$ is adequate for a communication system. The final thing that we observe is that for a small number of nodes the estimation of the jamming signal seems to be better than that of the information. The information signal u that we want to estimate is common for all nodes but the jamming signal is just a different term z_i which contains also the unknown channel h_{ji} for every node. That means that with the same two observations for every node we are estimating from set of two possible discrete BPSK values for u (effectively detecting the signal), and simultaneously we estimate $z_i = h_{ji}z$ (and not z which might also be a discrete modulated signal).

The MSE_{zi} has low values even for small N. As the number of nodes increases the observations from the different nodes for the information signal u increase leading to an MSE_u that is lower than MSE_{zi}. This is achieved for $N \geq 6$.

5.3 Results for MSE vs σ_z^2

In our next set of results we assume a constant number of nodes $N = 5$ and we vary σ_z^2 between 1 to 10. In figure 5.3 we observe that in the proposed system that we have two observations for every node, as σ_z^2 increases, both MSE_u, MSE_{zi} remain practically in the same low desirable value below 0.1. That means that our system is not vulnerable to jamming, and as the power of the jamming signal σ_z^2 increases the system responds and estimates the information signal u in a very efficient way. In figure 5.4 we observe the difference between the baseline and proposed system. Here as the σ_z^2 increases (power of jamming increases) we observe a massive increase in MSE_u and MSE_{zi}. These results illustrate the importance of the observations in (3.1) for every node. In the baseline system that we practically cannot use these observations we have only (3.2) for every node. That means that we have no more information for every z_i and when this jamming signal has higher power than the information signal we cannot isolate and estimate the later.

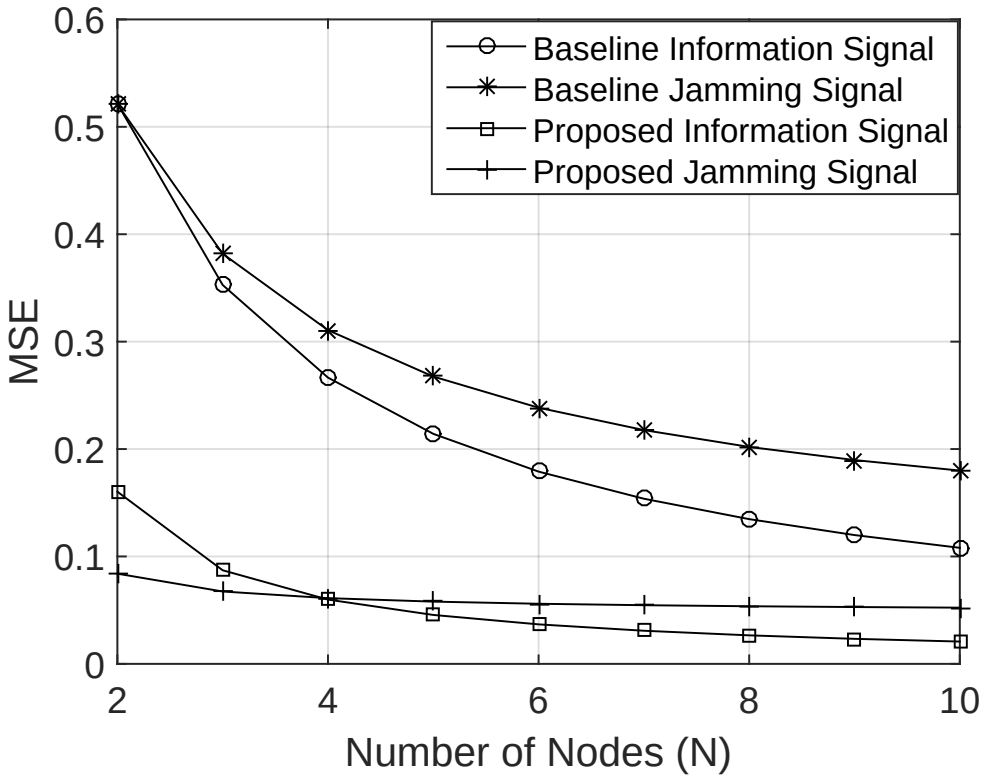

Figure 5.1: Results for the AWGN channel.

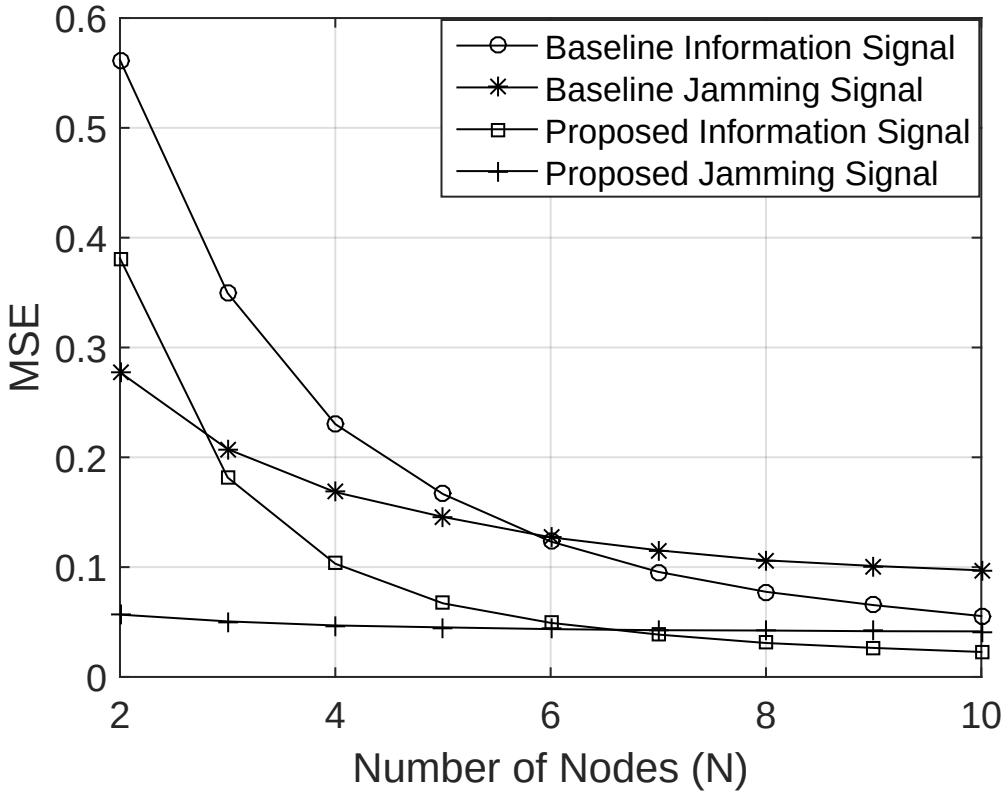

Figure 5.2: Results for the Rayleigh fading channel.

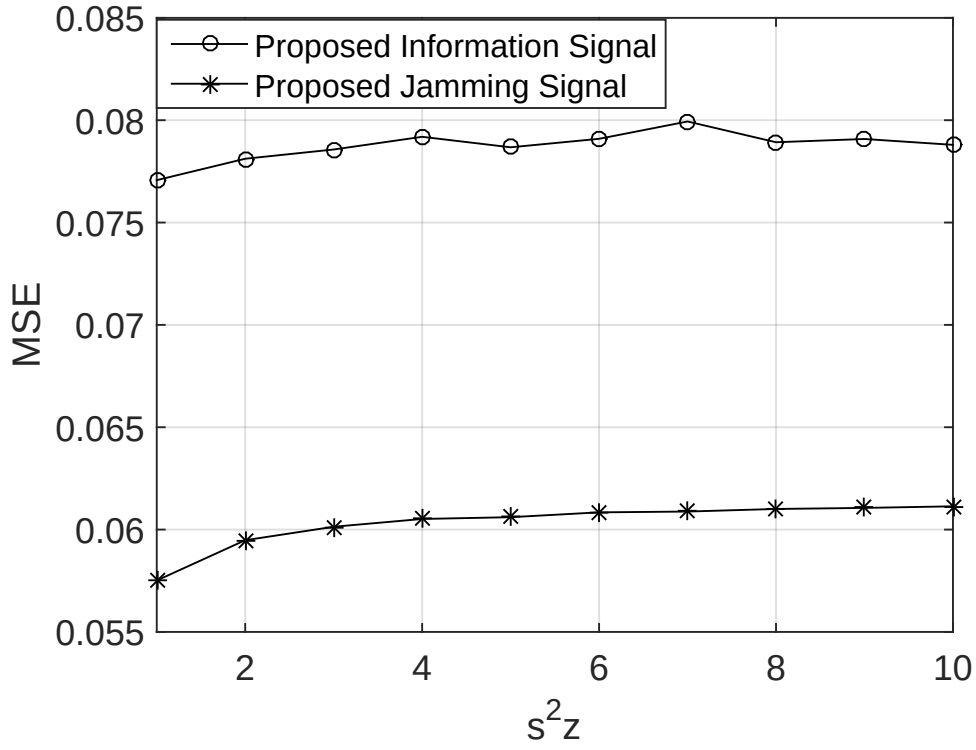

Figure 5.3: Power of the jamming signal increases in the proposed system for N=5.

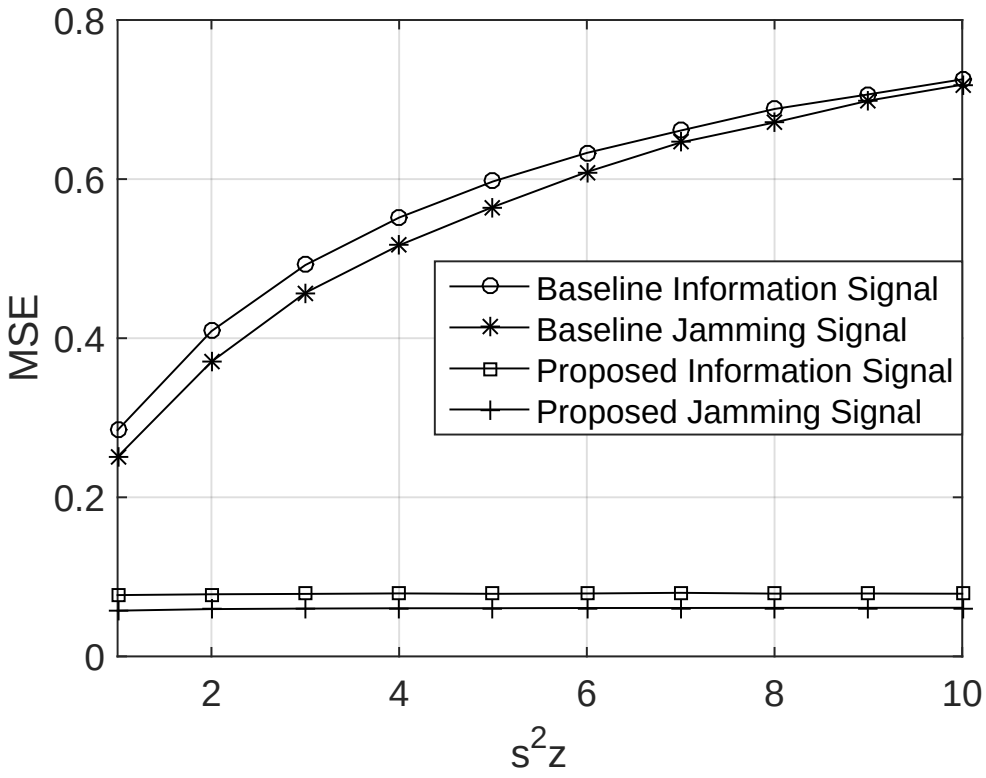

Figure 5.4: Power of the jamming signal increases in both systems for N=5.

Chapter 6

Conclusions

In this paper, we considered a network when a swarm of nodes receive an information signal from a master node and a jamming signal from an RF jammer. We proposed first a transmission scheme where the master node remains silent for a slot and second a joint data and and jamming signal estimation algorithm using LMMSE estimation. We derived analytical closed-form expressions for the MSE of our system. Our results indicate that as the number of nodes in the swarm increases estimation of both the jamming and information signals is improved significantly. Our results also showed that our system is robust against RF jamming attacks because as the power of jamming signal (σ_z^2) increases, the MSE_u and MSE_{zi} remains constant.

Bibliography

[1] D. Kosmanos, N. Prodromou, A. Argyriou, L. A. Maglaras, and H. Janicke, "Mimo techniques for jamming threat suppression in vehicular networks,"

[2] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of rf communicating vehicles using unsupervised machine learning," *Vehicular Communications*, vol. 13, pp. 56 – 63, 2018.

[3] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, pp. 41–47, May 2006.

[4] A. Argyriou and . Alay, "Distributed estimation in wireless sensor networks with an interference canceling fusion center," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 2205–2214, March 2016.

[5] A. S. A. Osanaiye Opeyemi and G. P. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors Basel Switzerland*, June 2018.

[6] H. A. B. Salameh, S. Almajali, M. Ayyash, and H. Elgala, "Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks," *IEEE Internet of Things Journal*, vol. 5, pp. 1904–1913, June 2018.

[7] T. S. Rappaport, *Wireless Communications Principles and Practice*. Dorling Kimdersley, 2009.

[8] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory*. Prentice Hall, 1993.

[9] B. Hajek, *Random Processes for Engineers*. 2014.

[10] I. Bahceci and A. Khandani, "Linear estimation of correlated data in wireless sensor networks with optimum power allocation and analog modulation," *Communications, IEEE Transactions on*, vol. 56, pp. 1146 –1156, july 2008.